## CSfC Selections for VPN Clients

VPN Client products used in CSfC solutions shall be validated by NIAP/CCEVS or CCRA partnering schemes as complying with the current requirements of NIAP's Protection Profile for IPsec VPN Clients, and this validated compliance shall include the selectable requirements contained in this document.

**CSfC selections for VPN Client evaluations:**

**FCS_CKM.1.1(1):** Refinement: The [selection: TOE, TOE platform] shall generate asymmetric cryptographic keys used for key establishment in accordance with

- *NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")*

**FCS_CKM.1.1(2):** Refinement: The [selection: TOE, TOE platform] shall generate asymmetric cryptographic keys used for IKE peer authentication in accordance with

- FIPS PUB 186-4, " Digital Signature Standard (DSS)", Appendix 8.4 for ECDSA schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves];

**FCS_COP.1.1(2):** Refinement: The [selection: TOE, TOE platform] shall perform cryptographic signature services in accordance with a specified cryptographic algorithm:

- FIPS PUB 186-4, " Digital Signature Standard (DSS)", Appendix 8.4 for ECDSA schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curve]]

**FCS_COP.1.1(3):** Refinement: The [selection: TOE, TOE platform] shall perform *[cryptographic hashing services]* in accordance with a specified cryptographic algorithm [SHA-256, SHA-384) and message digest sizes [256, 384] bits that meet the following: *FIPS Pub 180-4, "Secure Hash Standard."*

**FCS_I PSEC_EXT.1.1(1):** The [selection: TOE, TOE platfo rm] shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), 19 (256-bit Random ECP), 20 (384-bit Random ECPL and [selection: 5 (1536-bit MODP), 24 (2048-bit MODP with 256-bit POS), [assignment: other DH groups that are implemented by the TOE], no other DH groups].

**FCS_IPSEC_EXT.1.1 (2):** The [selection: TOE, TOE platform] shall ensure that all IKE protocols perform peer authentication using *[ECDSA]* that use X.509v3 certificates that conform to RFC 4945 and [selection: Pre shared Keys, no other method].

**FCS_RBG_EXT.1.2:** The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [selection: *a software-based noise source, a platform-based RBG]* with a minimum of *[256 bits]* of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.